SOLUTION BRIEF

Manufacturing Industry

Protect the modern operational technology environment against advanced attacks

OVERVIEW

The modern manufacturing operational technology (OT) environment has evolved to include more connected and networked endpoints, providing organizations with more automation, monitoring and control. However, unlike the endpoints found in the traditional IT environment—e.g., laptops, desktops and mobile devices—OT endpoints also include other networked devices such as robots, pumps, valves and sensors.

The industrial control system (ICS) that controls these processes runs in real time, is often aged or unsupported, rarely stops to install patches, and can lead to disastrous consequences if compromised. As new, unscreened executable files from many sources in the supply chain are introduced into the system, securing the integrity of the shop floor is difficult to maintain. In short, the OT environment has been built with the goal of optimizing productivity, not security.

Carbon Black's Next-Generation Endpoint Security solutions defend ICS and OT environments against advanced attacks targeting intellectual property. Carbon Black also enables manufacturers to disrupt adversarial behavior by identifying the root causes of attacks.

34% **of industrial control systems have been breached more than twice over the past 12 months**
[Source: SANS Institute, June 2015]

5–10 **The majority of embedded devices in industrial control systems are 5- to 10-years-old, and weren't built with cyber security in mind.**

3rd **Manufacturing is the third most breached industry**
[Source: 2015 Verizon Data Breach Investigations Report]

The Cyber Security Challenge in Today's Manufacturing World

Manufacturers face increasing attacks not only from cyber criminals but also from competitors and nation-states seeking to steal IP and other trade secrets. By connecting all manner of devices, regardless of location or type, manufacturers increase productivity, reduce costs and improve their ability to make smart, quick management decisions. However, continued reliance on antivirus solutions, aging hardware, and unsupported software environments opens the door to advanced attacks. Machine-to-machine connections, mobility and virtualization are now part of the factory floor and supply chain, so it is imperative that these endpoints and server connections are made with security in mind.

Security for the Extended Operational Environment

By preventing any unauthorized process from running on your endpoints and servers, Carbon Black Enterprise Protection prevents malware from exfiltrating corporate and customer data. Carbon Black's real-time approach to detection, prevention and response does not slow down operational or administrative systems.

Cyber Security Framework Alignment

Carbon Black's Next-Generation Endpoint Security platform helps you align with the most advanced cyber-security frameworks, such as the CIS Top 20 Critical Security Controls and NIST 800-53, to ensure coverage of the latest techniques.

Defense Against Portable Media Infections

Deploying Cb Protection's lightweight agent and setting a high-enforcement policy locks down the system and prevents unauthorized portable devices from accessing information or installing unapproved software or malware.

Extended Value of Legacy Infrastructure

Using application control to block unapproved processes from executing, Carbon Black Enterprise Protection enables you to keep unsupported and legacy operating systems in place, while maintaining a secure—and compliant—posture.

Carbon Black.

SUMMARY

Carbon Black provides the most advanced Next-Generation Endpoint Security platform available to help manufacturers prevent advanced attacks and identify threats across the ICS and OT environment. The Carbon Black Security Platform enables security teams to disrupt attacker behavior, optimize efficiency and productivity, and align with advanced cyber-security frameworks.

MANUFACTURERS LOOK TO CARBON BLACK

COMPANY ONE

A leading appliance manufacturer has the Windows XP operating system widely deployed throughout the enterprise. According to the CISO, many of the company's revenue-critical applications, including robotics, inventory control and accounting, can only run on XP machines. With the XP end-of-life deadline fast approaching, the company didn't want to purchase costly emergency Premium Support from Microsoft.

The Solution

The CISO chose Cb Protection to ensure that his XP-dependent machines would remain secure even though Microsoft support has now ended. Cb Protection was quickly deployed on 5,000 Windows XP endpoints to defend against advanced threats even though there are no more Windows XP patches, as well as to protect against previous and future exploits of XP vulnerabilities. The solution also delivered audit proof and historical intelligence to fuel compliance reports that demonstrate policy enforcement and provided continuous monitoring of all fixed-function Windows XP systems and business processes for indicators of compromise.

Results

The company dramatically improved its overall security posture and compliance standing while also significantly reducing its attack surface. With Cb Protection in place, they are no longer vulnerable to the host of possible exploits that could take advantage of the vulnerabilities associated with unsupported Windows XP machines.

COMPANY TWO

A Fortune 500 Company needed a highly scalable, enterprise-ready security solution that could give them fast, accurate visibility into and protection against a wide range of threats, today and in the future. Requiring fast deployment on more than 50K endpoints to protect them—and the critical information on them—against an expanding and increasingly sophisticated threat landscape. All organizations need malware protection, but a multinational company with a treasure trove of patents and other intellectual property is a highly desirable target for criminal organizations and nation-states looking to profit from others' work.

The Solution

A deployment of this size in such a tight timeframe might have scared off other security vendors, but not Carbon Black. All the installations were quickly completed and Cb Protection deployed on an average of 2,500 endpoints per day. At its completion, this was the largest deployment of an application control solution in a dynamic corporate environment anywhere in the world. Once the solution was fully deployed, we worked closely with the customer to put their endpoints into high-enforcement mode, which is appropriate for this customer because it blocks all untrusted software from executing unless the IT administrator approves it.

Results

The customer now enjoys the benefits of continuous monitoring and recording of all endpoint and server activity—in real time—to provide unique visibility into what's happening in the environment, as well as a full audit trail. The customer's CISO credited the strong partnership between his company and Carbon Black as the key to this successful implementation.

Carbon Black.

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

1100 Winter Street, Waltham, MA 02451 USA P 617.393.7400 F 617.393.7499 www.carbonblack.com